Securing network traffic and intrusion detection data

Benjamin D. Uphoff
Los Alamos National Laboratory
bduphoff@lanl.gov

Johnny S.K. Wong
Iowa State University
wong@cs.iastate.edu

Abstract

Networking devices and intrusion detection systems are capable of generating large volumes of audit information. This information should be considered sensitive, as it can be used by organizations for forensic investigations when a compromise of the network occurs. Privacy concerns must also be considered, as there are many legal and ethical issues with maintaining these types of data sets. Until now, little attention has been paid to protecting these data sets from attackers, both internal and external. This work provides solutions to this problem by describing the data integrity and user authentication mechanisms needed to properly secure network traffic and intrusion detection data sets within an intrusion detection framework.

Introduction

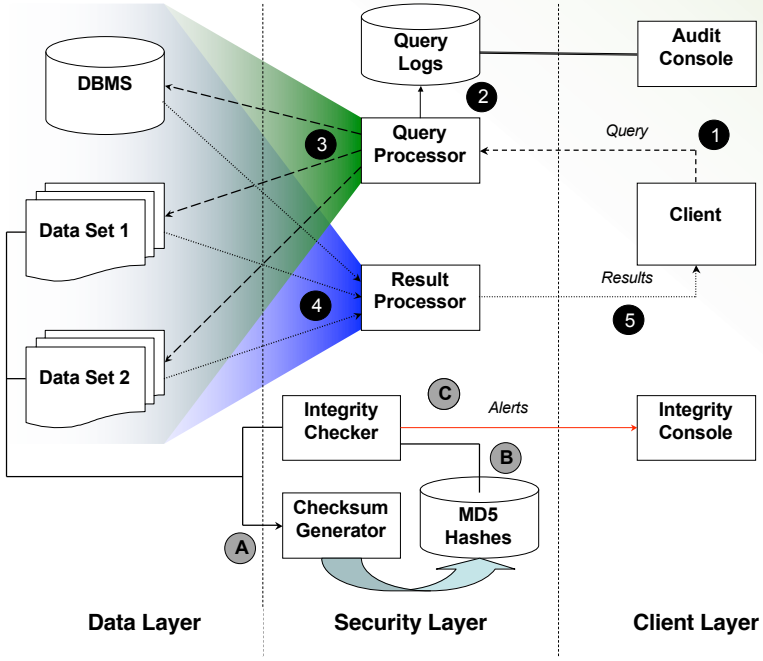
We present an integrated framework for the capture and retrieval of network security data sets that provides essential security features to protect sensitive data. Data integrity is monitored through the use of secure hashing functions. Access to data in the system is logged for audit purposes and restricted by way of a domain specific query language. We address the threats of both malicious insiders and external hackers by providing security measures for both scenarios.

Network security and intrusion detection data is captured in real-time and a MD5 checksum is generated. A daemon process continually computes the checksums of data files stored within the framework to compare against the original checksum.

To access data stored within the framework, client programs must authenticate using a custom XML-based query language. User credentials are mapped to access controls that are used to dynamically filter results returned to the client. As queries are received, they are logged in the system metadata so as to provide an audit trail of system use. This allows administrators to assure that those with legitimate access are not abusing their rights.

Additionally, all inter-process communications between clients and servers are performed over SSL to protect sensitive data in transit. System metadata is stored in a hardened relational database as a further security measure.

Intrusion Detection Framework Security Features



Authentication, Logging and Access Controls

1. Client submits query in XML, provides authentication information
2. Query processor authenticates the user, logs the query in the system metadata for auditing
3. Query is decomposed and parallel search is executed
4. Results from the query are returned to the result processor for filtering
5. Results are dynamically filtered with user-specific access controls and returned to the client application

Data Integrity Monitoring

- **A** Data is streamed to the checksum generator, which records a MD5 hash of each data file
- **B** The integrity checker periodically verifies the integrity of each data file by re-computing the MD5 checksum
- **C** If at any point the integrity check fails, the integrity checker sends an alert to a monitoring console

Query Example

```
<Query user="bob" password="l0gm31n">
  <SocketResult host="192.168.1.1" port="1234"/>
  <Query srcip="192.168.1.0~192.168.1..255" date="2004-9-1~2004-9-30"/>
  <Query dstip="192.168.0.0~192.168.255.255" date="2004-9-1~2004-9-30"/>
</Query>
```

In this example query, Bob requests data that from the 192.168 network be sent to a socket on a server listening on port 1234. As shown in table 1, the user has access controls restricting his access to data in the 192.168 subnet. The result processor will use these access controls to dynamically filter out data that does not match the access controls.

Before writing a record to the socket, the result processor filters the record based on the information in table 1. If the field values (i.e. *srcip* and *dstip*) are not valid based on this information then the result is not written to the socket. In this example, records returned to the result processor with a source IP of 192.168.1.50 will be filtered out according to the fourth access control entry in table 1.

User	Field	Access Control
bob	dstip	+192.168.1.0~192.168.1.128
bob	dstip	+192.168.11.0~192.168.11.255
bob	srcip	+192.168.1.0~192.168.1.128
bob	srcip	-192.168.1.50

Table 1. Access controls

Los Alamos NATIONAL LABORATORY EST.1943